U.S. Department of Justice

United States Attorney
Northern District of Illinois

Devlin N. Su
Assistant United States Attorney

Dirksen Federal Courthouse
219 South Dearborn Street, Fifth Floor
Chicago, IL 60604

Direct Line: (312) 886-0667
Fax: (312)353-4322
E-mail: devlin.su@usdoj.gov

December 9, 2019

Sami Ziad Azhari
Azhari LLC
30 N. LaSalle Street, Suite 2140
Chicago, IL 60602
Sazhari@azharillc.com

Michael Irving Leonard
LeonardMeyer LLP
120 North LaSalle, Suite 2000
Chicago, IL 60602
mleonard@leonardmeyerllp.com

***United States v. Michael Persaud*, No. 16 CR 793**

Dear Counsel:

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure, the government hereby notifies you that, at trial, the government intends to present expert testimony, as detailed below.

1. <u>Dr. John Levine</u>

The government intends to call Dr. John Levine to provide expert testimony regarding email transmission and spam marketing. Dr. Levine's *curriculum vitae* and a list provided by Dr. Levine of matters in which he has provided expert testimony are enclosed.

The government anticipates that Dr. Levine may testify that companies who host email services on behalf of users are often known as email providers. Examples of such email providers include large companies such as Comcast or Google, but may also include smaller companies. Email providers typically operate at least one email server connected to the internet, which routes emails from the sender to the recipient. Each email server typically has at least one unique Internet Protocol (IP) address associated with it, which helps identify that server to others. Once a user composes

and sends an email, that email is transmitted to an email server operated by the sender's email provider. That server then uses Simple Mail Transport Protocol (SMTP) to locate an email server operated by the recipient's email provider and inform that email provider about the email to allow the provider to determine whether it should deliver that email. Assuming that the answer is yes, that email is delivered to the recipient via the email server run by the recipient's email provider.

The government anticipates that Dr. Levine may define "spam" as email sent in bulk to recipients who do not want the email. Spam comprises the majority of emails sent in the world. The most common use of spam is to advertise commercial products and/or services, while the second-most common use of spam is to further fraud schemes. Spam is technically sent the same way as any other email, but that people who send spam ("spammers") commonly use computer programs that connect to email servers and send lots of emails very quickly. Spammers typically obtain recipient email addresses by buying lists of addresses, or guessing recipient addresses. Spammers typically make money in exchange for sending spam on behalf of others.

The government anticipates that Dr. Levine may testify that email providers and/or individual users commonly operate spam filters, which are computer programs designed to automatically detect whether an incoming email is spam. If the filter determines that the email is spam, the filter will automatically block the spam from the user's inbox. These filters apply automated rules to determine whether an incoming email is spam, including by looking at an email's technical characteristics (*e.g.*, whether it was sent from an email server in a different country known for sending spam), the email's contents (*e.g.*, whether there are patterns in the email's text that is more likely to occur in spam), and/or by consulting "blacklists" operated by various third parties. Blacklists are lists of IP addresses associated with email servers through which spam has been sent to complaining recipients, who have flagged given messages as spam. Once flagged, that spam can be traced to a specific email server through the spam's header data, and that email server's IP address reported to a blacklist. If an email server's IP address appears on a blacklist, then any spam filter who consults that specific blacklist will automatically block any emails sent by that server from reaching the recipient's inbox. Spammers commonly attempt to defeat spam filters in a variety of ways, including by arranging to route spam through different email servers or editing the spam's text.

Dr. Levine may testify that email providers typically have a rule, communicated to their users in the providers' terms of service, which prohibits using that email provider to send spam. The no-spam rule exists because once the IP address of an email provider's email server appears on any blacklist, then any spam filter consulting that blacklist will block any emails sent by that server. That would typically include any legitimate emails sent by other users of that email provider, who will experience error messages when they attempt to send emails. This would

typically cause legitimate users of that email provider to cancel their service with that provider—thereby causing the provider to lose revenue—and move to a different provider that does not operate a blacklisted email server. Accordingly, email providers typically prohibit users from using their email service to send spam because of the risk of lost revenues from their email servers being blacklisted. The consequences of violating this rule may ultimately include termination of that user's account with the email provider. Spammers may attempt to defeat the providers' no-spam rules through various methods, including by altering the timing of when they send spam relative to when they sign up for service, and by signing up for service from new email providers under a fake identity.

The bases of Dr. Levine's testimony are his training and experience. Dr. Levine is being compensated by the government at a rate of $400 per hour.

2. FBI Computer Forensic Examiner Kerry J. Kolecheck

The government intends to call Kerry J. Kolecheck, FBI Computer Forensic Examiner, as an expert in the field of computer forensics. Mr. Kolecheck has approximately ten years of experience as a computer forensic examiner at the FBI. As detailed in his enclosed *curriculum vitae*, Mr. Kolecheck obtained his A.D. as an Electronic Computer Technician from Gateway Technical College in 1987, and his B.S. in Industrial Engineering from the University of Wisconsin, Milwaukee in 1993. After working as an engineer from 1988 through 2004, he began his career at the FBI in a support role. In 2009, he began working as a computer forensic examiner on the FBI Milwaukee's Computer Analysis Response Team. Since 2009, he has completed approximately 35 computer and forensics-related courses; received approximately 10 certificates and awards; and given approximately 7 presentations in this field.

The government anticipates that Mr. Kolecheck may testify about the forensic analysis performed in 2016 of a Western Digital My Passport hard drive (the "WD Hard Drive") seized from defendant Michael Persaud in June 2016, including (1) a Dell Studio XP5 8000SE, serial number GR6YD51 and associated hard drives; (2) an Apple MacBook Air, serial number C02H60GCDRQ4, and associated hard drives; an Apple iMac, serial number D25N601YFLHH; (4) a Buffalo Linkstation LS-Q4, serial number 95824590505372, and associated hard drives; and (5) a Dell Studio XPS M1640, serial number 21F18J1, and associated hard drive (the "Electronic Devices"); including that forensic images were created of the Electronic Devices, that forensic images are a bit-for-bit copy of the Electronic Devices using specific imaging software, and that an MD5 hash algorithm was used to confirm the image was an exact duplicate of the Electronic Devices; and about the derivative evidence created of the Electronic Devices, based upon the review and selections made by the investigating FBI agent, which derivative evidence he will introduce into evidence at trial.

The government also anticipates Mr. Kolecheck may testify about his examination of the images of the Electronic Devices, including the computer and user names associated with each device, browser search history, IP addresses assigned to the each device, IP addresses accessed from each device, text, Word, Excel, and PDF documents created or accessed from each device relevant to defendant's spam campaigns, spam emails sent, financial records, instructional videos on how to send spam, and identification information and emails for Michael Pearson and Jeff Martinez.

* * *

We recognize our obligation for continuing disclosure pursuant to Rule 16, and request reciprocal expert disclosures from you pursuant to Federal Rule of Criminal Procedure 16(b)(1)(C). Should we receive any additional information relating to these experts, we will supplement our disclosures accordingly. Please do not hesitate to contact us if you have any questions or concerns.

Very truly yours,

JOHN R. LAUSCH, JR.
United States Attorney

By: */s/ Devlin N. Su*
Shoba Pillay
Devlin N. Su
Assistant United States Attorneys

Enclosures